

# Apple Bytes

The Newsletter of the Lynchburg Apple Core

Volume 2006.04 ----- Lynchburg, VA -----April 8, 2006

## April Meeting

**General meeting is at Lynchburg College, Thursday, April 20, 7:00 PM.**

The April meeting at **Lynchburg College, room 14 Hopwood Hall** will begin with a general discussion and Q&A session at 7:00 p.m. followed by the featured presentation.

This month Frank Land will present his experience with the new Intel chip Macs. Frank has an Intel iMac.

*NOTE: There are several hyperlinks in this month's Apple Bytes. They have been tested in Reader 7.05 as well as Preview 3.04 and found to work. You should be able to click on them to go open your web browser and go the web page. If you have trouble with them, please let editor Tom Johnson or President Michael Corbin know.*

=====

### Backing Up Your Data

Michael Corbin presented several backup strategies at the March meeting, including the ultimate: creating a software RAID (level 1, mirrored), which, it turns out Macs can do inexpensively (Michael built an external Firewire one for about \$200, and might have been able to do for as little as \$40 adding an internal drive and catching the right sale), but which can only be done with expensive hardware on a Windows system, and then not for a boot drive on any version except XP Pro.

Different methods of backing up your data were discussed. Some software packages designed to do this include Synchronize Plus and ChronoSync (will keep two computers synchronized). SuperDuper works like Carbon Copy Cloner and is also shareware that clones your hard drive to another drive. Split & Concatenate can save a disk image to multiple DVD's for archival backup.

The way Macs function makes them more amenable to booting up from another hard drive, such as a clone of your hard drive. Windows computers look for a floppy disc on bootup, and if that is not found looks for a designated hard drive to boot from. Macs search for any bootable drive.

In the old days of OS-9, you could drag and drop the icon of the system file into any hard drive to install that system and make that hard drive bootable. You can't do that today with OS-X. OS-X has a lot of invisible files that don't install this way. For this reason, cloning is needed to make a backup of your operating system and all the installed applications. Hard drives have become downright cheap these days (of course, cheap is relative). Best Buy recently had a 320 Gigabyte hard drive for \$190 with a \$60 rebate. If you are going to work with your extra hard drive on a daily basis, you may not want to go for the cheapest. However, if it will be used several times a year to back up data files, the el-cheapo may be the way to go. Note: if you are looking for an internal drive, make sure you get either an ATA or SATA drive, whichever your model uses, as they are not interchangeable.

Another thing to remember, Macs will not boot up from any USB drive! Make sure any external hard drive you get for your Mac is a FireWire drive if you want to boot up from it. The USB drive can store data, but the whole reason of cloning to another drive is to boot up from the backup drive and restore a faulty or crashed hard drive.

Now for the ultimate back up scheme: the RAID. Redundant Array of Independent Devices means the

computer writes to two drives simultaneously making an instant back up drive. Neat, you don't have to do anything, the data is stored on another drive (or two, three, however many drives you want).

Here is how you do this. It is best if the two drives have the same size (otherwise the larger will only be used to the capacity of the smaller drive). They should also be formatted the same. Plug the empty (ie, devoid of data) drives into your Mac. Open **Applications**, then **Utilities** and launch **Disk Utility**. Select one of the drives and you will see a tag at the top of the **Disk Utility** window that says **RAID**. Select that. You will see places to name your RAID, to format the RAID volume ("Mac OS Extended Journaled" is recommended, it is the default). Then you choose the RAID type. You want "Mirrored RAID Set". Then just drag the images of the two hard drives *in the left column of the Disk Utility window* into the center window and your Mac will create a RAID and the new image will appear as one single hard drive. Drag files, copy, work from files within this image and you duplicate everything on both drives. Neat!!

Michael has working copies of his digital photos in process stored on his RAID system and all of his work on the photos is automatically stored on both drives. If one drive crashes, he still has everything backed up and only has to replace the bad drive and he is back in business. (It should be noted that as a professional photographer, his archived photos are on several hundred CDs and DVDs.)

- Tom Johnson, Editor



## One Step To Safer Computing

By Jacob Loeb

As Mac users, we are greatly protected from some of the perils of the online world. To date, OS X has not suffered from any major Trojan, worm, Spyware, or virus. Vulnerabilities in OS X have been only theoretical exploits that are quickly patched, or are infections that relied on gross user error. I, as do many experts, discourage Mac owners from using an anti-virus program because they are unneeded. We all need to remember that change is the only constant, but by just adjusting one setting, you can make your Mac nearly impervious to any future online attack.

The bottom line is, to stay protected in the future, stop working from your Administrator account. Most Mac users don't know there are a least four levels of user accounts available in Mac OS X. The most powerful of those accounts is "root" and this account is all-powerful. Root users can do anything on an operating system including destroying it. That is a little too much power for any user to have, so Apple rightfully turns this account off and requires it to be activated in a less than straightforward way.

Root is good to know about, but you really don't need to use it because, chances are, you already have plenty of power by running as "Administrator." If you only have one user account on your Mac (usually the one set up when you first booted up the computer), then you are running as Administrator. Administrator user accounts are almost as powerful as Root and have just as much ability to cause damage. You should care about what level your user account is running at, because a malicious program can do almost anything you can do. Windows users suffer from this; often it is the cause of major PC problems. In the Windows world, users have to run as Administrator in order for all their software to work. Unlike the Mac OS, Windows users rarely have to enter the password in order to make changes or install software, good or bad. So a Windows user can install something without being asked for permission. The Mac user is better off because they are asked for the Administrator's password for almost everything they do in OS X.

Instead of potentially facing the problem Windows users have, you should run your user account at the lower level of "Standard," instead of Administrator. Standard user accounts own their account contents and settings within that account. They can't install or delete anything outside of the user account without using an Administrator's password. Now this may seem limiting, but it's not very different than what you are accustomed

to. Unlike a "limited" user account you would use for young children, a standard account has full use of every application and feature on the computer. The only big difference is to make changes to the system or install new software, you will have to enter an administrator username and password.

Every system has to have one Administrator account to work properly. To make this user account change, it's easiest just to create a new Administrator account and downgrade your current one to Standard. Here is what you do in Mac OS 10.4, but other versions of Mac OS are similar. To start, open "System Preferences" and Click on "Accounts." You may need to click on the padlock icon in the lower right corner of the window. Enter your password and click OK. Above the padlock icon is a pair of "+" and "-" buttons. Click on the "+" to add a new account. A pop down menu will appear for you to enter in the new user's information. I name this account "Admin" because Administrator takes me too long to type, but if you are fast at typing feel free to do the whole thing. Next skip down to Password and enter a good password that you can remember. It should be different than your current user account password. Retype it in the "Verify" text field and then put a Password Hint in if you want. Please do not put your password in the Password Hint section; you would be shocked how many times I see that. The last step before you click the "Create Account" button is to put a check in the checkbox marked "Allow user to administer this computer."

Now you have two administrator accounts on your computer, so all that's left is to change your account to the Standard level. Click on your account listed in the left hand pane of the Accounts system preference window. Now click on the Password tab and look for the checkbox that says "Allow user to administer this computer." Uncheck it and you will be asked for an Administrator user name and password. Enter the user name and password for the account you just set up and click OK. You are now a Standard level user.

The only difference you will notice as a Standard level user is that you need to enter a username and password, where before you just needed to provide a password. Most everything other than that will be the same. It's free computer prevention, and it's a small price to pay for the added the security you'll have. But this step and any other protective measure will all go to waste if you are quick to enter your Administrator Password or do so without thinking. You should expect to give it when installing trusted software or changing a system setting but never enter it to look at an email/iChat attachment. Pay attention which application you give your Administrator password to. Is it friend or foe? Knowing the difference will prevent you from ever having to suffer the worst user experience: a computer packed full of Spyware, Trojans, worms, and viruses - experiences just like many Windows users have now.

reprinted with permission from Jacob Loeb

To see this article online, [click here](#)

=====

## From the Earthlink Newsletter

### File Encryption

#### Protect your privacy!

Losing a laptop, or having it stolen, can make your heart freeze. Not only are you out a thousand bucks (or more), but suddenly a stranger can read your email, see your income tax files, and maybe admire your company's top-secret strategy for the next year. But you have a great tool to protect that data from prying eyes: file encryption. When files are encrypted, only people with the password can use or read them. It's the absolute best way to maintain your privacy if someone nasty gets their little hands on your computer.

#### What does file encryption software do?

Encryption software takes data, like your tax files (or your 007 mission profile), and encodes it so that no one can read it without the "key" (associated with your password). This code, like the key, is created using a mathematic algorithm that we can't explain here (because we don't understand it ourselves!). But once created, it's very secure and any person or computer trying to look at your file just sees a bunch of gobbledygook. Then,

once you've signed in to your computer to do your taxes (or attack the evil fortress), the software turns all the gobbledygook back into recognizable form.

In most cases, it's not hard to set up and you never need to worry about all the math.

### **I already use a password to sign in. Is this different from file encryption?**

Using a password to sign in is a good idea, but it's not encryption, and it's not as powerful. A password will help block bad guys from getting into your operating system (like Windows XP or Mac OS X). In most cases, that could be enough, because the average run-of-the-mill thief may not bother going further than that. But a professional thief, making his living from credit card numbers or company secrets, may have a few more tricks up his sleeves. For one thing, though the password protects access to your operating system, it doesn't stop anyone from physically removing your hard drive (which contains all your data) from your computer. Once they hook up your hard drive to a different computer, they can see whatever they want. Unless the files on the hard drive are encrypted, that is. If they're encrypted, then there's not a thing a thief can do.

### **Really? Not a thing the thief can do?**

Well, never say never, but today's best encryption software is powerful stuff. If a thief bothered to try and crack the code (and had a government computer to help), it could still take millions of years or more to do the job. Even including time spent waiting on hold, that's probably enough time to cancel your credit cards.

### **A Caveat...**

While encryption keeps your files safe from prying eyes, it doesn't really keep them safe from being tampered with. If you recover a stolen computer, you can't be completely sure that your data still says what it used to. If it's critical information, throw it away and use your back-up data. (You did back up your data, right?)

### **But do I really need millions of years of protection?**

Maybe not! If your computer never leaves your house, and you use it for family emails and photos, you may not want to bother with encryption. But if you use a laptop, keep files with company (or personal) secrets, or are generally concerned about privacy, you should think seriously about protecting your data. Another consideration is how often you forget passwords. Encryption is powerful, and usually the only way to unencrypt a file is to use the password. If you forget the password, that data is gone. Forever.

### **Enough theory. How do I encrypt?**

If you have Windows XP Pro or Mac OS X, encryption is already built in, and you just have to turn it on (see how below). In fact, you won't even have to remember another password, because your operating system sign-in password will automatically control the encryption. HINT: Encrypting and unencrypting files can slow down your computer. So if you like editing video footage or music on your computer, you might want to store those files in a place that's not encrypted.

To encrypt your files:

#### **Mac OS X:**

Mac OS X allows you to encrypt your entire Home folder at one time.

1. From the Apple menu, choose System Preferences.
2. Click the Security icon to open the Security preference panel.
3. Choose Turn On FileVault.

Mac OS X will sign you out of your profile, then will work for a while, encrypting your entire Home folder. The next time you sign in, your files will automatically be unencrypted and ready to use. If you don't sign in, no one will be able to read any of your personal files.

## Earlier Windows or Mac OS systems:

If you're using an earlier version of Windows or Mac OS (or XP Home), you may have to install some third-party encryption software, such as PGP.

To see this article online [click here](#)

=====  
PGP is primarily known for the ability to encrypt email as well as single files. Paid/registered versions also enable the making of encrypted disk images, which decrypt on the fly very quickly and reliably. A similar capability is built into Disk Utility, which also makes encrypted disk images. The article below explains why you should care about encryption.

## Why I wrote PGP

by Phil Zimmerman

excerpted from the documentation for PGP 6.5 (currently in version 9)

*"Whatever you do will be insignificant, but it is very important that you do it."*

—Mahatma Gandhi.

It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance. Or you may be communicating with a political dissident in a repressive country. Whatever it is, you don't want your private electronic mail (email) or confidential documents read by anyone else. There's nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution.

The right to privacy is spread implicitly throughout the Bill of Rights. But when the United States Constitution was framed, the Founding Fathers saw no need to explicitly spell out the right to a private conversation. That would have been silly. Two hundred years ago, all conversations were private. If someone else was within earshot, you could just go out behind the barn and have your conversation there. No one could listen in without your knowledge. The right to a private conversation was a natural right, not just in a philosophical sense, but in a law-of-physics sense, given the technology of the time.

But with the coming of the information age, starting with the invention of the telephone, all that has changed. Now most of our conversations are conducted electronically. This allows our most intimate conversations to be exposed without our knowledge. Cellular phone calls may be monitored by anyone with a radio. Electronic mail, sent across the Internet, is no more secure than cellular phone calls. Email is rapidly replacing postal mail, becoming the norm for everyone, not the novelty it was in the past. And email can be routinely and automatically scanned for interesting keywords, on a large scale, without detection. This is like driftnet fishing.

Perhaps you think your email is legitimate enough that encryption is unwarranted. If you really are a law-abiding citizen with nothing to hide, then why don't you always send your paper mail on postcards? Why not submit to drug testing on demand? Why require a warrant for police searches of your house? Are you trying to hide something? If you hide your mail inside envelopes, does that mean you must be a subversive or a drug dealer, or maybe a paranoid nut? Do law-abiding citizens have any need to encrypt their email?

What if everyone believed that law-abiding citizens should use postcards for their mail? If a nonconformist tried to assert his privacy by using an envelope for his mail, it would draw suspicion. Perhaps the authorities would open his mail to see what he's hiding. Fortunately, we don't live in that kind of world, because everyone protects most of their mail with envelopes. So no one draws suspicion by asserting their privacy with an envelope. There's safety in numbers. Analogously, it would be nice if everyone routinely used encryption for all their email, innocent or not, so that no one drew suspicion by asserting their email privacy with encryption. Think of it as a form of solidarity.

Until now, if the government wanted to violate the privacy of ordinary citizens, they had to expend a certain amount of expense and labor to intercept and steam open and read paper mail. Or they had to listen to and possibly transcribe spoken telephone conversation, at least before automatic voice recognition technology became available. This kind of labor-intensive monitoring was not practical on a large scale. It was only done in

important cases when it seemed worthwhile.

Senate Bill 266, a 1991 omnibus anticrime bill, had an unsettling measure buried in it. If this non-binding resolution had become real law, it would have forced manufacturers of secure communications equipment to insert special “trap doors” in their products, so that the government could read anyone’s encrypted messages. It reads, “It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.” It was this bill that led me to publish PGP electronically for free that year, shortly before the measure was defeated after vigorous protest by civil libertarians and industry groups.

The 1994 Digital Telephony bill mandated that phone companies install remote wiretapping ports into their central office digital switches, creating a new technology infrastructure for “point-and-click” wiretapping, so that federal agents no longer have to go out and attach alligator clips to phone lines. Now they will be able to sit in their headquarters in Washington and listen in on your phone calls. Of course, the law still requires a court order for a wiretap. But while technology infrastructures can persist for generations, laws and policies can change overnight. Once a communications infrastructure optimized for surveillance becomes entrenched, a shift in political conditions may lead to abuse of this new-found power. Political conditions may shift with the election of a new government, or perhaps more abruptly from the bombing of a federal building.

A year after the 1994 Digital Telephony bill passed, the FBI disclosed plans to require the phone companies to build into their infrastructure the capacity to simultaneously wiretap 1 percent of all phone calls in all major U.S. cities. This would represent more than a thousandfold increase over previous levels in the number of phones that could be wiretapped. In previous years, there were only about a thousand court-ordered wiretaps in the United States per year, at the federal, state, and local levels combined. It’s hard to see how the government could even employ enough judges to sign enough wiretap orders to wiretap 1 percent of all our phone calls, much less hire enough federal agents to sit and listen to all that traffic in real time. The only plausible way of processing that amount of traffic is a massive Orwellian application of automated voice recognition technology to sift through it all, searching for interesting keywords or searching for a particular speaker’s voice. If the government doesn’t find the target in the first 1 percent sample, the wiretaps can be shifted over to a different 1 percent until the target is found, or until everyone’s phone line has been checked for subversive traffic. The FBI says they need this capacity to plan for the future. This plan sparked such outrage that it was defeated in Congress, at least this time around, in 1995. But the mere fact that the FBI even asked for these broad powers is revealing of their agenda. And the defeat of this plan isn’t so reassuring when you consider that the 1994 Digital Telephony bill was also defeated the first time it was introduced, in 1993.

Advances in technology will not permit the maintenance of the status quo, as far as privacy is concerned. The status quo is unstable. If we do nothing, new technologies will give the government new automatic surveillance capabilities that Stalin could never have dreamed of. The only way to hold the line on privacy in the information age is strong cryptography.

You don’t have to distrust the government to want to use cryptography. Your business can be wiretapped by business rivals, organized crime, or foreign governments. Several foreign governments, for example, admit to using their signals intelligence against companies from other countries to give their own corporations a competitive edge. Ironically, the United States government’s restrictions on cryptography have weakened U.S. corporate defenses against foreign intelligence and organized crime.

The government knows what a pivotal role cryptography is destined to play in the power relationship with its people. In April 1993, the Clinton administration unveiled a bold new encryption policy initiative, which had been under development at the National Security Agency (NSA) since the start of the Bush administration. The centerpiece of this initiative was a government-built encryption device, called the Clipper chip, containing a new classified NSA encryption algorithm. The government tried to encourage private industry to design it into all their secure communication products, such as secure phones, secure faxes, and so on. AT&T put Clipper into its secure voice products. The catch: At the time of manufacture, each Clipper chip is loaded with its own unique key, and the government gets to keep a copy, placed in escrow. Not to worry, though—the government promises that they will use these keys to read your traffic only “when duly authorized

by law.” Of course, to make Clipper completely effective, the next logical step would be to outlaw other forms of cryptography.

The government initially claimed that using Clipper would be voluntary, that no one would be forced to use it instead of other types of cryptography. But the public reaction against the Clipper chip has been strong, stronger than the government anticipated. The computer industry has monolithically proclaimed its opposition to using Clipper. FBI director Louis Freeh responded to a question in a press conference in 1994 by saying that if Clipper failed to gain public support, and FBI wiretaps were shut out by non-government-controlled cryptography, his office would have no choice but to seek legislative relief. Later, in the aftermath of the Oklahoma City tragedy, Mr. Freeh testified before the Senate Judiciary Committee that public availability of strong cryptography must be curtailed by the government (although no one had suggested that cryptography was used by the bombers). The Electronic Privacy Information Center (EPIC) obtained some revealing documents under the Freedom of Information Act. In a briefing document titled “Encryption: The Threat, Applications and Potential Solutions,” and sent to the National Security Council in February 1993, the FBI, NSA, and Department of Justice (DOJ) concluded that “Technical solutions, such as they are, will only work if they are incorporated into all encryption products. To ensure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to Government encryption criteria is required.”

The government has a track record that does not inspire confidence that they will never abuse our civil liberties. The FBI’s COINTELPRO program targeted groups that opposed government policies. They spied on the antiwar movement and the civil rights movement. They wiretapped the phone of Martin Luther King Jr. Nixon had his enemies list. And then there was the Watergate mess. Congress now seems intent on passing laws curtailing our civil liberties on the Internet. At no time in the past century has public distrust of the government been so broadly distributed across the political spectrum, as it is today.

If we want to resist this unsettling trend in the government to outlaw cryptography, one measure we can apply is to use cryptography as much as we can now while it’s still legal. When use of strong cryptography becomes popular, it’s harder for the government to criminalize it. Therefore, using PGP is good for preserving democracy.

If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have access to good cryptographic technology. So do the big arms and drug traffickers. But ordinary people and grassroots political organizations mostly have not had access to affordable “military grade” public-key cryptographic technology. Until now.

PGP empowers people to take their privacy into their own hands. There’s a growing social need for it. That’s why I created it.

---

## **Mac Boot Camp** (copied from Apple’s Web Announcement)

More and more people are buying and loving Macs. To make this choice simply irresistible, Apple will include technology in the next major release of Mac OS X, Leopard, that lets you install and run the Windows XP operating system on your Mac. Called Boot Camp (for now), you can download a public beta today. As elegant as it gets, Boot Camp lets you install Windows XP without moving your Mac data, though you will need to bring your own copy to the table, as Apple Computer does not sell or support Microsoft Windows.(1) Boot Camp will burn a CD of all the required drivers for Windows so you don't have to scrounge around the Internet looking for them.

### Run XP natively

Once you’ve completed Boot Camp, simply hold down the option key at startup to choose between Mac OS X and Windows. (That’s the “alt” key for you longtime Windows users.) After starting up, your Mac runs Windows completely natively. Simply restart to come back to Mac.

### What you’ll need

\* Mac OS X Tiger v10.4.6 (check Software Update)

- \* The latest Firmware update (check Support Downloads)
- \* 10GB free hard disk space
- \* An Intel-based Mac
- \* A blank recordable CD
- \* A printer for the instructions (You'll want to print them before installing Windows, really.)
- \* A bona fide installation disc for Microsoft Windows XP, Service Pack 2, Home or Professional (No multi-disc, upgrade or Media Center versions.)

### The Boot Camp course

Boot Camp Public Beta provides a straightforward means of letting your Mac run Windows. Here's how it works:

Space maker. Meet the most elegant hard drive utility ever.

\* First, you need to make sure your Intel-based Mac has the latest version of Mac OS X and the latest firmware update. These provide technologies that make Boot Camp possible. It's also wise to print out the Installation & Setup Guide.

\* The Boot Camp burns a CD with the drivers Windows needs to recognize Mac-specific hardware. It is very important to do this before starting the Windows installation.

\* The software also helps you set aside hard drive space for the Windows installation, without moving any of your Mac files around. Just drag the intuitive slider to choose the size that's right for you. Boot Camp also helps you remove the Windows partition, should you so desire.

\* Next, insert your Windows installation disc, restart and follow the Windows installation process. The only tricky part is selecting the C: drive manually. Be sure to get this right, or you could erase your Mac files accidentally. Remember, Apple Computer does not sell or support Microsoft Windows.

\* After the installation process is complete and your Mac has booted Windows, you'll need the Macintosh Drivers CD you burned previously. When you insert the CD, it will automatically install the drivers. Follow the instructions in the Installation & Setup Guide for helpful hints.

\* Don't forget to follow best practices for updating and protecting your Windows system.

1. You'll need Windows XP Home Edition or Professional, Service Pack 2 installation disc.

### Included Amenities

For your convenience, Boot Camp burns a CD with all the Mac-specific drivers for Windows:

- \* Graphics
- \* Networking
- \* Audio
- \* AirPort wireless
- \* Bluetooth
- \* The Eject key (on Apple keyboards)
- \* Brightness control for built-in displays

This CD also installs a Startup Disk control panel for Windows. To find it, look for Startup Disk in the Performance and Maintenance section of the Windows XP Control Panel. See the Installation & Setup Guide for more details.

## Using Windows on a Mac

Mac hardware operates differently from PCs, and this public beta does not support all features of the Mac in Windows.

## Mac OS X Leopard

Developers can learn all about the sixth major release of Mac OS X this century at Apple's Worldwide Developer Conference, to be held August 7-11 in San Francisco.

## EFI and BIOS

Macs use an ultra-modern industry standard technology called EFI to handle booting. Sadly, Windows XP, and even the upcoming Vista, are stuck in the 1980s with old-fashioned BIOS. But with Boot Camp, the Mac can operate smoothly in both centuries.

## Word to the Wise

Windows running on a Mac is like Windows running on a PC. That means it'll be subject to the same attacks that plague the Windows world. So be sure to keep it updated with the latest Microsoft Windows security fixes.

## Tell a Friend

Email people you think might be interested in Boot Camp for Intel-based Macs.

## Feedback

Please provide [bootcamp@apple.com](mailto:bootcamp@apple.com)feedback to improve future versions of the software.

=====

## Mac Tip of the Week

(Excerpted from [Mac OS X Tiger Killer Tips](#) by Scott Kelby).

### Easy Main Menu Access During the Movie

A must-know keyboard shortcut is how to get back to the main DVD menu while the DVD is already playing. To get there, just press Command-~ (that's the Tilde key just above the Tab key), and it will cycle you back to the DVD's main menu.

=====

The Spring 2006 Mac OS X Class was completed with nearly a "full house"

The latest Mac OS X Class was held at CVCC in the Graphic Arts Mac Lab with 14 in attendance, almost reaching the class limit of 15. It was held over three Saturday mornings to try to improve over the rush of the schedule of classes held in the past. There was lively interchange between the class members and instructor Gordon Mattox, who fielded many questions about Mac operations. Chris Smith and Frank Land contributed a lot to discussion as did Ed Bolen and Tony Young.

Several people were taking the course for the third time to catch up on new features and to brush up on their understandings. In response to requests in the past, Gordon developed a three-page listing and explanation of the more common and useful keyboard commands. He will send it to anyone requesting it by e-mail.

This will be the last class Gordon teaches at CVCC since he is moving to Roanoke, but he said he would be glad to answer questions via phone or e-mail.

=====

# May Meeting:

Lynchburg College, Hopwood Hall - Thursday May 16, - 7:00 PM

7:00 to 7:30, open questions time; bring us a problem to solve

Topic: favorite freeware and shareware!

Bring a blank CD-R or RW and we'll all share

=====

Visit the Lynchburg Apple Core Web Site for Updates, Information, and Important Links:

<http://www.lynchburgmug.org>